An XDR Primer: The Promise of Simplifying Security Operations

Contents

Introduction

When you think of a Security Operations Center (SOC), what comes to mind? A room full of ninjas triaging alerts? Or does a large room filled with massive threat maps come to mind?

Security operations is arguably one of the toughest jobs in the industry. Over the years, an organization's SOC has continued to grow in both importance and complexity as a byproduct of digital transformation and adoption of newer tech.

A recent ESG report tells us that more than half of organizations use more than 26 different commercial, homegrown, or open-source tools for security operations.[1] Adopting new technology should make the SOC team's job easier, but often this isn't the case.

The impact of connectivity

As a result of hybrid work and cloud adoption, we're more connected now than ever before. Businesses are operating as integrated ecosystems where boundaries between corporations, customers, suppliers, and partners blur. This new age of interconnectedness – though beneficial to our business and private lives – has led to an expanding attack surface and a rise in sophisticated cyberattacks.

We know it's tempting to just buy the latest technology to address new security concerns. But the reality is without a solution that can streamline the security stack, adding more tools just creates more confusion in an already disjointed security environment. Which can lead to more security gaps that slow you down, when the real goal is to accelerate detection and prioritize response.

"To be truly effective, cybersecurity vendors must be open to sharing data and context so that advanced analytics across as many vectors as possible can rapidly detect and respond to the world's most sophisticated threat actor groups."

AJ Shipley
VP of Product Management for Threat Detection and Response

Time is money

Let's face it, when it comes to security, time is money. It takes a company an average of 277 days to discover and contain each breach. That means your business could have a thief walking around undetected, accessing internal applications, and stealing private data every day for almost 10 months – that's unacceptable!

Security analysts do their best to sort and prioritize thousands of alerts each day hoping to find the most effective approach to threat detection and remediation; but most struggle. To truly solve these problems, we have to consider the root causes of an ineffective security team:

1. **Poor integration with existing security investments**

   Most companies rely on tools from multiple vendors to build out their entire security infrastructure, meaning they tend to have several stand-alone solutions with little to no integration or shared telemetry. When solutions aren't working together, it has a snowballing effect.

   Bad integration limits the amount of telemetry and intelligence shared, making it impossible to create a single, context-rich view. If you can't see all the threats across the entire enterprise, how can you effectively mitigate risks at scale, or even at all?

   Cisco's AJ Shipley, VP of Product Management for Threat Detection and Response, said it best, "For years, cyber adversaries have exploited any advantage possible to further their motives, including the inability, due to lack of data sharing, to effectively correlate multiple low fidelity signals across multiple vendors into a highly accurate detection. To be truly effective, cybersecurity vendors must be open to sharing data and context so that advanced analytics across as many vectors as possible can rapidly detect and respond to the world's most sophisticated threat actor groups." Security teams need an open and extensible approach so their solutions work better together.

2. **Alert overload**

   ESG's recent SOC modernization study cites that 37% of IT and security professionals admitted their security operations are more difficult to manage in 2022 than just two years earlier due to the increasing volume and complexity of security alerts. Analysts are struggling to strike a balance between not only identifying the right threats but also prioritizing them in a way that helps determine the best remediation strategy to minimize the impact to their business.

   When analysts don't have adequate threat intelligence or contextual awareness, it's almost impossible to prioritize threats according to business impact. The result is a flood of alerts with no way to accurately distinguish which might tank your company by $5 million if overlooked or which may have little to no impact at all.

3. **Skills shortage**

   Further exacerbating the effects of siloed systems and alert fatigue on security operations is the shortage of analysts with the skillset needed to balance out responsibilities. According to ESG, 81% of IT and cybersecurity professionals agree that their security operations have been impacted by the global cybersecurity skills shortage.[2]

   Companies need a way to upskill their analysts to ensure the right actionable insights are discovered and emphasized so sophisticated threats don't go undetected or unaddressed. Integrated global and local threat intelligence helps close this gap by providing the additional context needed to accurately flag and prioritize threats for your team. This elevates every analyst's awareness of which threats are high risk and should be addressed immediately to improve security efficacy, making your team more effective regardless of their experience

XDR is Shifting the paradigm

As threats become increasingly sophisticated, the old detection and response model built upon self-contained point security solutions doesn't go far enough. Teams have turned to solutions like SIEM and SOAR to attempt to unify siloed environments and reduce alerts, but the problem remains. Today's security teams need a solution that transforms data from a range of sources into reliable alerts and insights so that they can act quickly with confidence.

In the last couple of years, Extended Detection and Response, better known as XDR, has gained momentum as an emerging technology that shows promise for filling the void with an open and unified approach to prevent, detect, and respond to threats quickly and efficiently.

But what exactly is XDR? In a nutshell, it's a solution that collects telemetry from multiple security tools into a central data repository, analyzes the collected and homogenized data to arrive at a detection of maliciousness, and accelerates response and remediation of that detected maliciousness. With an effective XDR, it's easier for analysts – regardless of tier – to focus on comprehensive threat detection, prioritized risk-based incident response, and improving productivity.

According to ESG's study, 51% of professionals say the security tools they currently use struggle to detect and investigate advanced threats.[2]

A risk-centric XDR solution leverages global threat intelligence and local context to quickly quantify, verify, and prioritize threats.

Correlate data to detect the most sophisticated threats anywhere

There's a lot to protect when you consider all the data that lives across your networks, endpoints, emails, and applications.

We know that a vast majority of organizations leverage a multi-vendor security stack to investigate and respond to threats. Isolated, these solutions can only provide partial visibility into what's happening at any given time, but when brought together this data turns into actionable and useful insights.

Act on what truly matters, faster

Every business is different. Depending on which systems and operations are most critical to your business, a threat festering for too long in the wrong place can stain your brand's reputation or lead to financial ruin. And to make matters worse, analysts often don't have the time to accurately prioritize the mountain of alerts they see daily.

A risk-centric XDR solution, however, leverages global threat intelligence and local context to quickly quantify, verify, and prioritize threats according to the probability of material risk. Essentially, XDR translates the unified global and local context to visualize the complete attack continuum and help analysts understand both the root cause and full scope of impact.

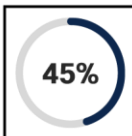
Five key elements of XDR done right

1. Provides prioritized and actionable telemetry, everywhere you need it
2. Enables unified detection, regardless of vector or vendor
3. Supports fast, accurate threat response
4. Offers a single investigative viewpoint for a streamlined user experience
5. Provides opportunities to elevate productivity and strengthen security posture

Optimize efficiencies to maximize value and accelerate outcomes

Outside of adversaries, the main enemies of security are limited context, skillsets, and time. But with a unified XDR console, even resource- and time-constrained teams can dramatically decrease dwell time.

The XDR approach of aggregating security data into a central location makes it easier for your teams to analyze, prioritize, and respond to the most critical threats with speed and accuracy regardless of their experience level. Built-in orchestration and automation helps teams offload repetitive tasks and direct limited resources to where they are most needed.



Organizations with a mature XDR implementation saw a improvement in security resilience compared to those without it.[3]

The journey to security resilience

Today, uncertainty is a guarantee. In response, companies are investing in resilience across every aspect of their business. But without the infusion of security resilience, your business may be vulnerable to unpredictable threats and changes.

As part of an open, integrated platform called Cisco Security Cloud, our XDR solution embeds security resilience across even the most complex hybrid multi-cloud environments. As more solutions are plugged into your XDR, you're able to strengthen detection and perform more complete response actions across all necessary vectors.

Why Cisco XDR?

At Cisco, our customers are at the core of everything we do. That's why we offer a comprehensive XDR solution with an extensive library of third-party integrations featuring leading security vendors to provide maximum flexibility.

We also know the last thing you need is more complexity, so we've created an all-in-one console for you – enabling your security and SOC analysts to detect, investigate and remediate threats in just a few clicks. Our solution is open, extensible and cloud-first so you can optimize your existing security investments and unify security detection across your entire environment.

[1]"ESG Complete Survey Results: SOC Modernization and the Role of XDR," Enterprise Strategy Group (ESG), September 2022 https://www.esg-global.com/research/esg-complete-survey-results-soc-modernization-and-the-role-of-xdr

[2]"SOC Modernization and the Role of XDR," Enterprise Strategy Group (ESG), June 2022 https://www.cisco.com/c/en/us/products/security/soc-modernization-xdr.html

[3] "Security Outcomes Report, Volume 3," Cisco, December 2022 https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C95-3551078-00 04/23